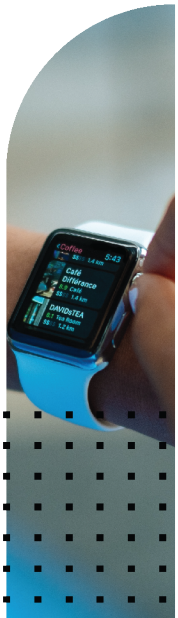
Release Notes

FortiSwitchOS 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 4, 2021
FortiSwitchOS 7.0.0 Release Notes
11-700-674489-20210504

TABLE OF CONTENTS

Change log

Date	Change Description
April 15, 2021	Initial release for FortiSwitchOS 7.0.0
May 4, 2021	Updated the “Common vulnerabilities and exposures” section.

Introduction

This document provides the following information for FortiSwitchOS 7.0.0 build 0022.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.0.0 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1048D, FS-1048E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.0

Release 7.0.0 provides the following new features.

GUI changes

- You can now configure Protocol Independent Multicast (PIM) version-4 routing in the GUI.
- You can now configure IPv6 static routes in the GUI.
- The average traffic bandwidth is now listed in the Traffic (Last Day) column in the *Physical Switch Ports* page (*Switch* > *Port* > *Physical*), *Physical Port Interfaces* page (*Switch* > *Interface* > *Physical*), and *Trunk Interfaces* page (*Switch* > *Interface* > *Trunk*) . You can now sort this column by value.
- The diagnostics monitoring of QSFP+ transceivers is now supported in the GUI (*Switch* > *Monitor* > *Modules*).
- You can now create or customize an ACL service by going to *Switch* > *ACL* > *Service*.

CLI changes

- You can now control whether the size of the layer-2 table is checked and how often. When the table size is more than 75-percent full or less than 70-percent full, FortiSwitchOS adds a warning to the system log.
- The factory default setting for power over Ethernet (PoE) pre-standard detection is now `disable` for both managed and standalone FortiSwitch units. When you upgrade FortiSwitchOS, the setting of PoE pre-standard detection stays the same. The setting of PoE pre-standard detection might change during a downgrade from FortiSwitchOS 7.0.0 to earlier versions.
- More protocols have been added to the `set protocol` command (under `config router setting`). You can now filter by any IPv6 protocol, IPv6 BGP, IPv6 IS-IS, IPv6 OSPF, IPv6 RIP, or IPv6 static. The `connected` option is no longer supported.
- You can now set up the following SNMP v3 notifications (traps):
  - The CPU usage is too high.
  - The configuration of an entity was changed.
  - The IP address for an interface was changed.
  - The available log space is low.
  - The available memory is low.
- The diagnostic monitoring interface (DMI) now detects the interface type (Short Reach or Copper Reach) and forward error correction (FEC) state for a module and displays this information with the `diagnose switch physical-ports list <port_name>` command.
- By default, the 25G and 100G ports of the FS-1048E and FS-3032E models now automatically detect whether FEC is supported by the module.
- Flow export and tracking have been improved. You can control how often the template is exported and specify a Berkeley packet filter (BPF).
- Virtual routing and forwarding (VRF) is now supported by DHCP relay (IPv4), bidirectional forwarding detection (BFD) for static routes (IPv4 and IPv6), link monitor (IPv4 and IPv6) on VRF-enabled switch virtual interfaces (SVIs), and OSPF (IPv4).
- VRF is now supported by the 500-Series switches.
- When you specify a route map during routing configuration, only the route maps for that protocol are listed.
- You can now use the alias CLI commands to grant an administrator access to individual configuration attributes, table entries, or CLI commands.

- Fortinet now supports Federal Information Processing Standard Publication (FIPS) 140-2 (Level 2) for the following FortiSwitch models:
  - FS-424E
  - FS-424E-FPOE
  - FS-M426E-FPOE
  - FS-424E-Fiber
  - FS-448E
  - FS-448E-FPOE
  - FS-1048E
  - FS-3032E
- The Media Redundancy Protocol (MRP) is now supported on the FSR-112D and FSR-124D models.
- When 802.1x authentication is being used, you can now move an 802.1x client between ports that are not directly connected to the FortiSwitch unit.
- The following RADIUS attributes are now supported for configuring dynamic non-native VLANs:
  - Egress-VLANID
  - Egress-VLAN-Name
  - Ingress-Filters

GUI and CLI changes

- You can now configure multiple flow-export collectors
- You can now configure multiple sFlow collectors.
- sFlow is now supported on the FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.
- The maximum number of IGMP-snooping groups has been increased. The following table lists the maximum number of groups for various FortiSwitch models:

FortiSwitch Models	Snooping Table Limit (values have been rounded)
FS-108E and FS-124E	500
FSR-112D-POE, FS-124F, FS-148E, FS-148F, FS-224E, FS-248D, FS-248E, FS-424D, FS-424E, FS-424E-Fiber, FS-426E, FS-448D, FS-448E	1,000
FS-1024D and FS-1048D	4,000
FS-3032D	6,000
FS-524D, FS-548D, 1048E, and 3032E	8,000

REST API changes

The following are the new REST API endpoints:

- The new `cmdb/system.alias/command` endpoint grants an administrator access to individual configuration attributes, table entries, or CLI commands.

- The new `cmdb/system.alias/group` endpoint bundles different alias commands together for easy assignment.
- The new `cmdb/router/vrf` command supports virtual routing and forwarding (VRF).

The schema for two REST API endpoints has changed:

- The schema for the `cmdb/system/sflow` endpoint has changed because you can now configure multiple sFlow collectors.
- The schema for the `cmdb/system/flow-export` endpoint has changed because you can now configure multiple flow-export collectors.

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Downgrading FortiSwitchOS 7.0.0 to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 to 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 to FortiSwitch 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitch 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitch 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.0.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See https://docs.fortinet.com/document/fortiswitch/6.4.3/managed-switch-release-notes.

Product integration and support

FortiSwitchOS 7.0.0 support

The following table lists FortiSwitchOS 7.0.0 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
609939	When the SNMP sever polls the switch for the SNMP attribute msgAuthoritativeEngineBoots, the switch returns 0.
621628	When there are parity errors, the FS-448D model has a high CPU usage.
666841	Setting the STP state on the port of a managed switch causes a memory leak.
670281	STP flaps for the ICL when it is part of a three-site FortiLink redundancy topology.
672607	The GUI does not force users to change their password on the first login.
673673	When a trusted host has been added to the administrator profile, the user cannot log in to the FortiSwitch CLI or GUI from FortiCloud.
675444	The fan speed of the FS-1048E was very high when the switch was running FortiSwitchOS 6.4.3.
678608	The FS-3032 and FS-1048 models have intermittent high traffic use in the internal interface.
680477	The timezone of the managed FortiSwitch unit is not synchronized with the timezone of the FortiGate device.
682442	Do not use FCLF8521P2BTL and FCLF852XP2BTL modules. They are not supported and can cause issues on the FortiSwitch unit. To find supported modules, refer to the FortiSwitch-Compatible Transceivers matrix.
682642	FortiSwitchOS sometimes does not communicate with the BCM PSE controller.
683831	The daemon for 802.1x port-based authentication crashed on the FS-448D-FPOE model.
684986	When a three-tier FortiLink MCLAG topology was configured, secondary FortiSwitch units in tier-2 and tier-3 go offline unexpectedly.
685954	When an Asian language (such as Japanese, Korean, or Chinese) is configured, the browser-based console stops responding.
686172	Jumbo frames are not supported on managed FortiSwitch units.
687104	802.1x authentication stops suddenly on the FS-148E model.
687698	The quarantine VLAN changed from 4093 to 2 on a managed FortiSwitch unit.
687889	Remote login to FortiSwitch Cloud does not work when trusthost is configured for the user logging in remotely.

Bug ID	Description
688024	There is a high packet loss when a FortiGate device is managing switches in an MCLAG-ICL topology.
689572	When FortiGate units in HA mode are managing FortiSwitch units, there are intermittent ping drops to the gateway.
689854	The session is removed after reauthentication when 802.1x port-based authentication with MAB enabled is configured.
689959	The 10G DAC link failed on an FS-148F model.
693991	The SFP module FG-TRAN-LX-C does not work well with the FSW-224E-POE model.
694302	When the FSR-112D model is in FortiLink mode, it does not forward multicast traffic to its uplink port.
696552	802.1x RADIUS authentication stops working randomly on a managed FS-108E model.
700800	When managed switches were upgraded from 6.2 to 6.4.6, some FS-112D-POE stayed offline until DHCP snooping was disabled.
700934	The average per interface value for the last day and the last week should not be the same.
701196	The root port for an Multiple Spanning Tree Protocol (MSTP) configuration was flapping.
703982	The PoE port mapping changed.
703985	An IP phone connected to port1 was delivering power to port8 instead.

Common vulnerabilities and exposures

FortiSwitchOS 7.0.0 is no longer vulnerable to the following CVEs:

- CVE-2021-26111
- CWE-1104

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.
606044	The value for cable length is wrong when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and

Bug ID	Description
	FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
610149	The results are inaccurate for open and short cables when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
617755	The internal interface cannot obtain IPv6 addresses with dhcpv6-snooping enabled on the native VLAN.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
704377	After adding and then removing `ip6-allowaccess ping` from a VRF-enabled switch virtual interface (SVI), ping is still allowed through.

www.fortinet.com